Directory Services

Session 813

Directory Services

David M. O'Rourke
Server Engineering Manager

Overview

- Apple's Open Directory
- Review of Open Directory and Mac OS X 10.1
- Future Plans for Jaguar
- Questions and Answers

Open Directory

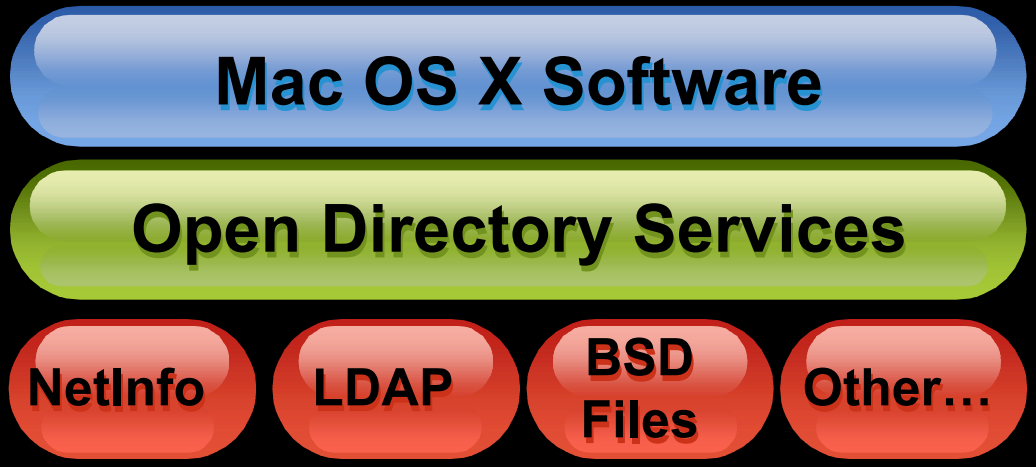
- New name—Includes
    - Client access, Directory Servers
- Combines industry standard protocols and open access technology
- Existing solutions shipped with Mac OS X and Mac OS X Server
- Open Source as part of Darwin

What Is Open Directory?

- Open Directory Access
  - Mac OS X Directory Services
  - lookupd for BSD code
- Directory Server Technology
  - OpenLDAP integrated with NetInfo
- Integrated tools for managing Directory Contents
  - Server and Desktop all based on Open Directory Technologies

What Is Directory Services?

- Part of Open Directory
  - An architecture that allows access to any Directory System
  - Includes read/write API and plug-in architecture



Mac OS X 10.1 Directory Services

- Includes:
  - LDAPv2 and NetInfo Clients
  - Documentation for integration with third-party LDAP servers
    - Active Directory White Paper
      http://www.apple.com/macosx/server
- Documented access API and plug-in API
  - SDK posted with sample code
  - Headers installed in
    /System/Library/Frameworks/DirectoryService.framework

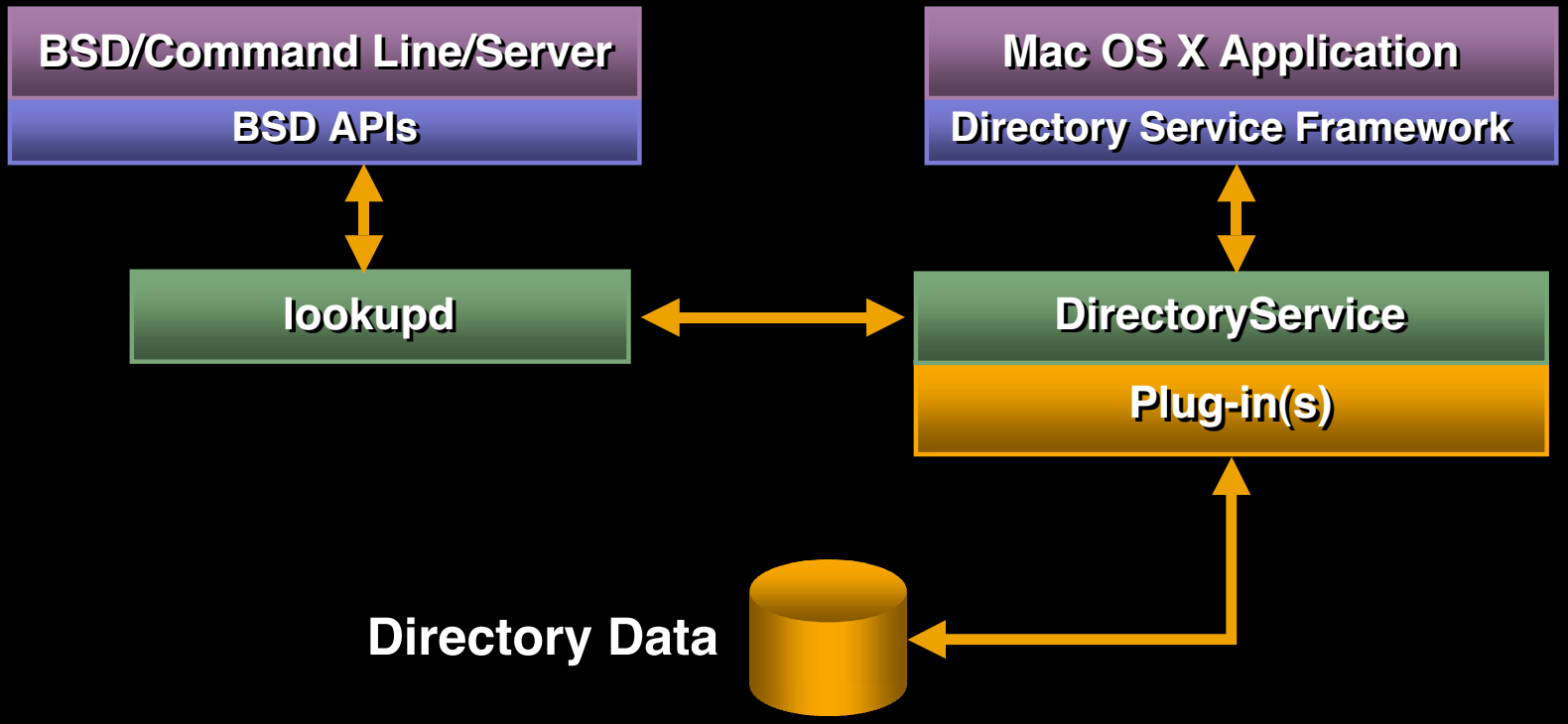
Mac OS X 10.1 Directory Server

- Mac OS X includes a powerful directory service called NetInfo
- Part of Darwin
- Provides both stand-alone and shared network configuration repository

Mac OS X 10.1 Directory Tools

- Mac OS X Server Administration Tools
- NetInfo Manager
    - Allows direct editing of NetInfo
- NetInfo Domain Setup
- Command-line tools
    - nidump, niload, nigrep, nicl and others

How Mac OS X 10.1 Uses Open Directory



Open Directory and Jaguar

Jaguar

- Open Directory Access will support
  - LDAPv3, BSD /etc files and more
- Jaguar includes OpenLDAP
  - Server and Client
  - Allows maximum compatibility for LDAP and legacy NetInfo clients
- New authentication options for password management

Enhancements We Will Cover Today

- Open Source
- Directory Proxy
- LDAPv3 and related features
- BSD Configuration files plug-in
- Authentication support for Mac OS X
- Service Discovery in Jaguar

Open Source, Directory Proxy, LDAP

Ken Witzke
Senior Software Engineer

Open Source

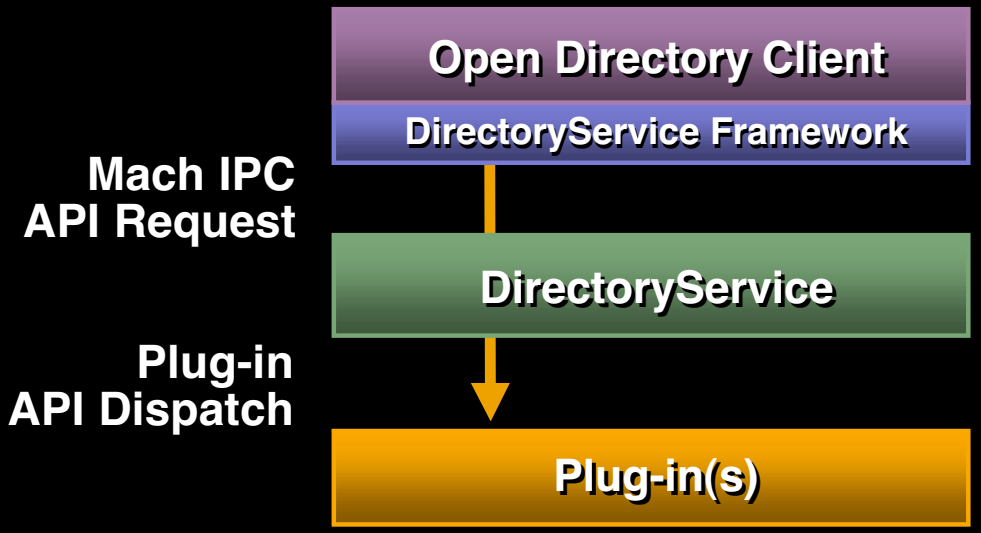
- Part of Darwin today (May 9th, 2002)
  - **http://www.apple.com/darwin**
  - DirectoryService
    - API Framework and daemon
  - LDAPv2, NetInfo, and Search Policy
- Jaguar
  - DSAgent for lookupd
  - LDAPv3 plug-in
  - BSD Configuration file plug-in
    - Read only
  - Service Discovery plug-ins

Directory Proxy

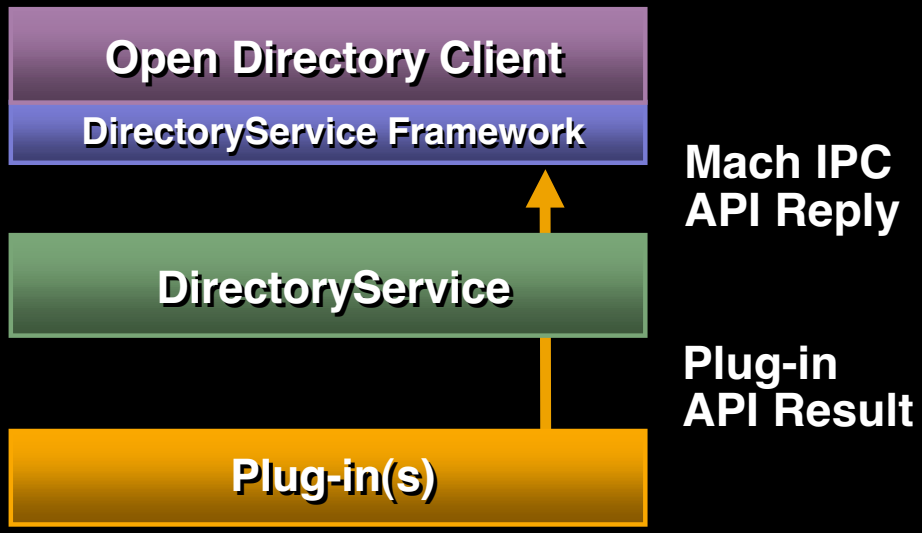
Directory Proxy

- Allows remote administration/access
    - Example: a remote server CPU in a networking closet
- Facilitates addition of remote access functionality to existing Open Directory-based software
- Helpful to understand API dispatch models

Local Dispatch Model



Local Dispatch Model



Proxy Dispatch Model

Machine A accesses Open Directory on Machine B

Open Directory Client

DirectoryService Framework

A

B

DirectoryService

Plug-in(s)

Proxy Dispatch Model

Machine A accesses Open Directory on Machine B

Open Directory Client

DirectoryService Framework

A

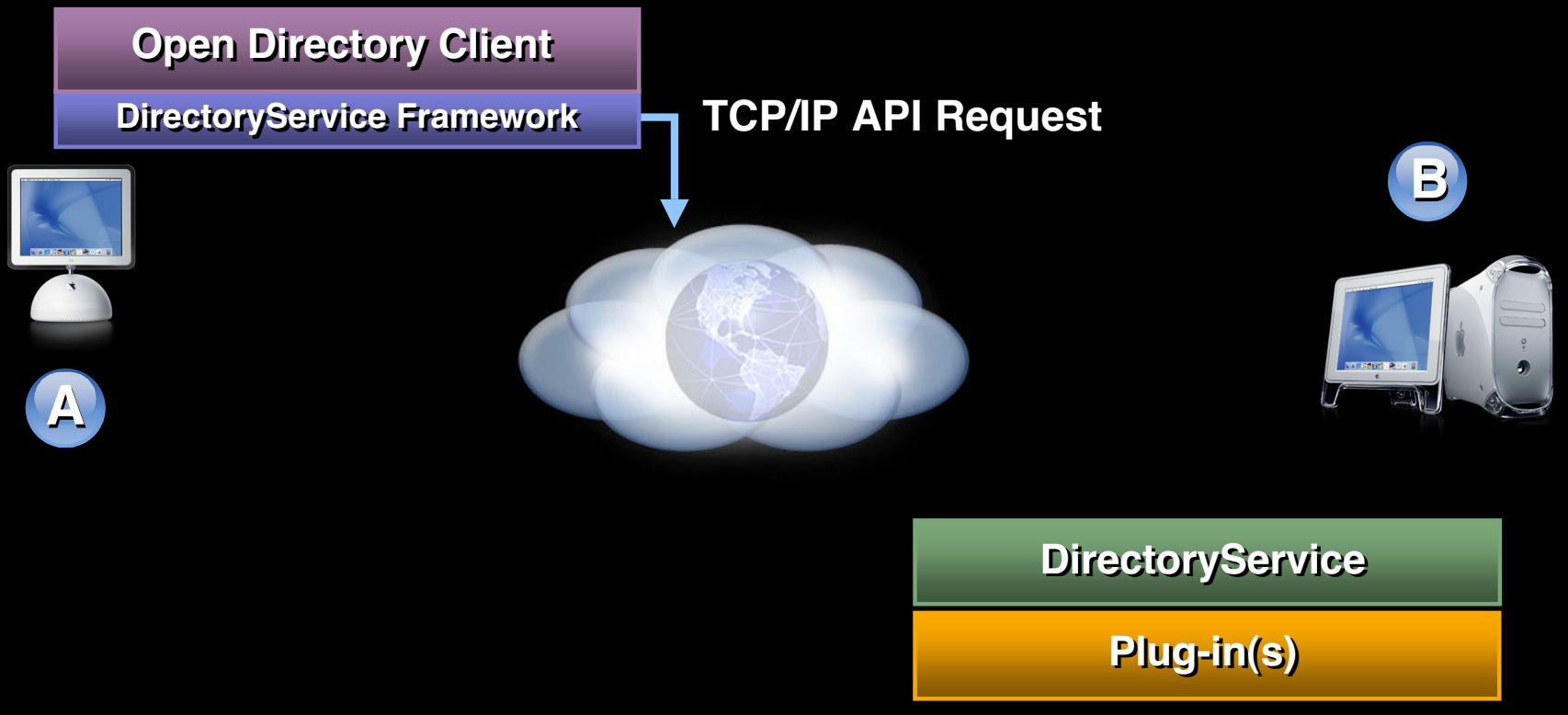
B

DirectoryService

Plug-in(s)

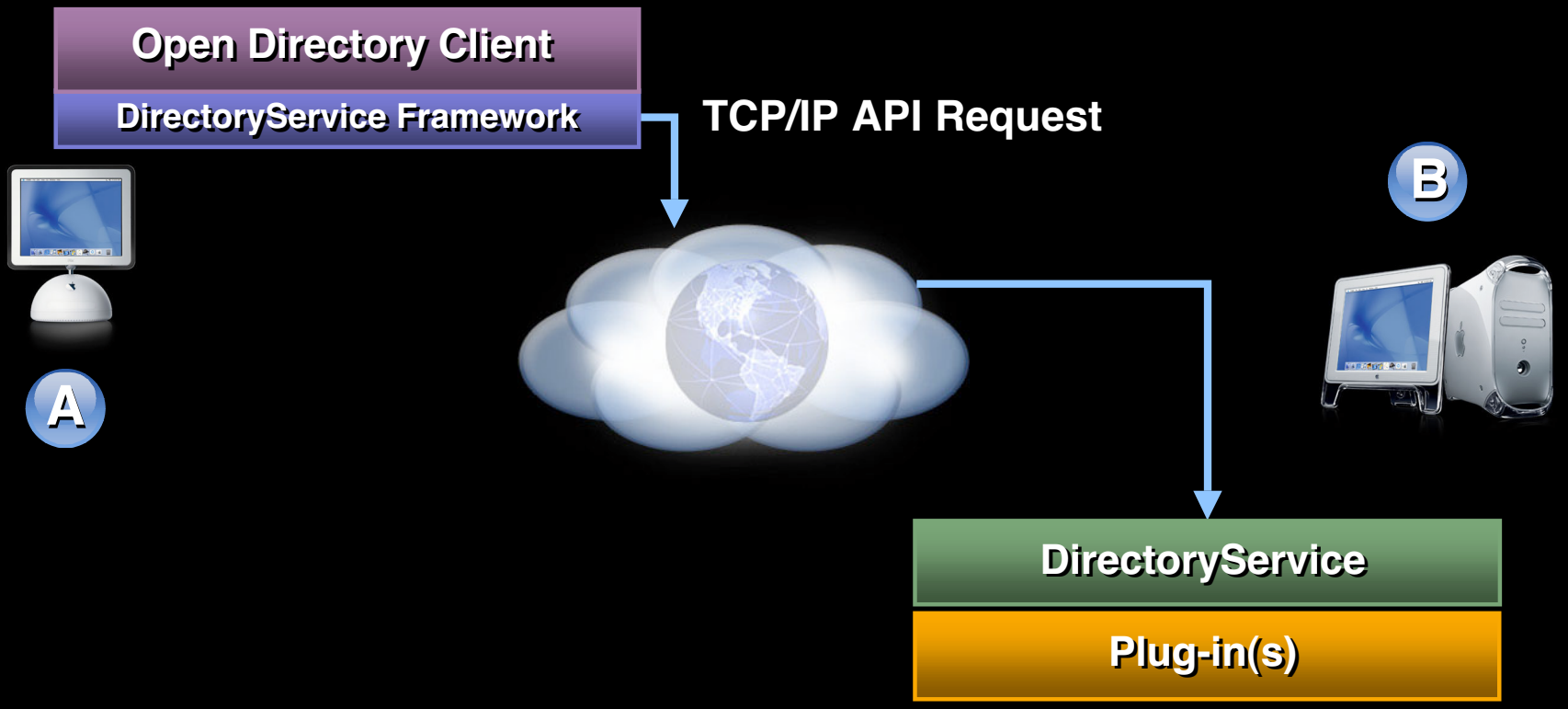
Proxy Dispatch Model

Machine A accesses Open Directory on Machine B



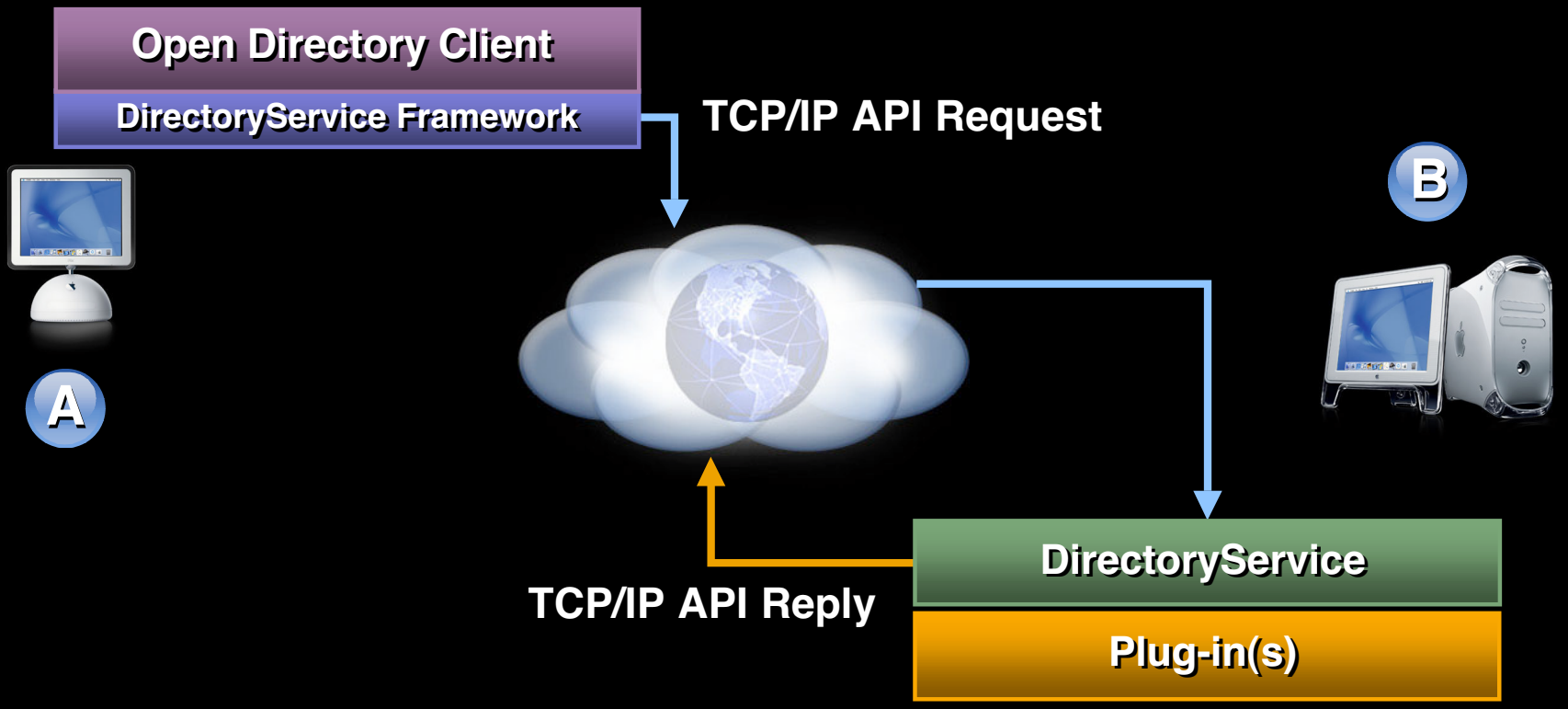
Proxy Dispatch Model

Machine A accesses Open Directory on Machine B



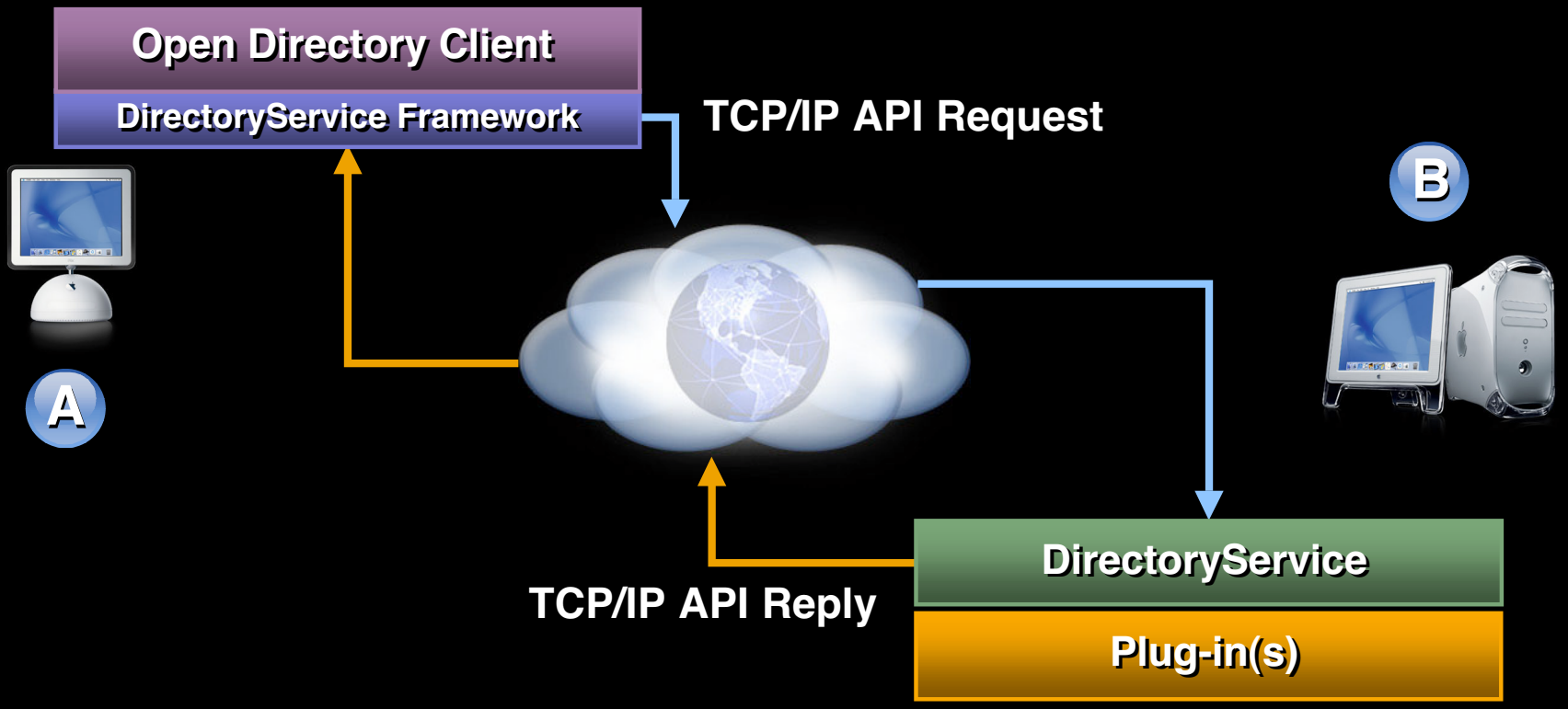
Proxy Dispatch Model

Machine A accesses Open Directory on Machine B



Proxy Dispatch Model

Machine A accesses Open Directory on Machine B



Directory Proxy Details

- Fully encrypted and authenticated
  - 128-bit encryption
  - Only local administrators are allowed to access the proxy connection
- Add proxy support to your application by replacing only the dsOpenDirService() call
  - All other code stays the same

Client Pseudo Code

Local (top) / Proxy (bottom) Models

```
myResult = dsOpenDirService(&myAPIRef);
myResult = dsOpenDirNode(myAPIRef,
                         &myDirNodeRef, …);
…
```

```
myResult = dsOpenDirServiceProxy(&myAPIRef, …);
myResult = dsOpenDirNode(myAPIRef,
                         &myDirNodeRef, …);
…
```

LDAP

Jaguar LDAP Client

- LDAPv3 read/write and SSL
- Minimized configuration setup
- Expanded record type definition
    - Better support for complex schemas
- OpenLDAP server on Mac OS X

Central Management of LDAP Clients

- DHCP and server-based mapping is a zero-configuration story for LDAP
- Support DHCP Option 95
  - DHCP server supplies LDAP URL(s) to all DHCP clients
- LDAP server-based configuration
  - Centralized management of LDAP client configuration

Expanded Record Type Definition

- Allows support for complex LDAP schemas
  - Full LDAP objectclass support
  - Record Type specific attribute mappings
  - Record creation capability
    - Auto-populate LDAP schema **must** have attributes with default values

OpenLDAP Server in Jaguar

- Version 2.1.x
  - Jaguar version based on 2.1
  - All changes will be released back to source tree
- LDAPv3 compliant
- Shared data store
  - LDAP and NetInfo use the same data store
  - Migration for existing NetInfo configurations

Demo

Jason Townsend

Authentication and Service Discovery

Jason Townsend
Software Engineer

Authentication in Jaguar

Moving beyond crypt passwords

- Mac OS X 10.1 based on crypt passwords
  - Stored crypt in NetInfo
- Jaguar will support additional forms of password verification
  - Replacement for crypt with >8 character support (MD5)
  - Mac OS X Password Server
  - Kerberos-based authentication

Password APIs

Use these APIs instead of getpwnam() and crypt()

- Security Framework
  - Password verification
  - Standard Aqua user experience
- PAM—Pluggable Authentication Modules
  - Linux/Solaris/BSD adopted APIs
- Directory Services—most flexible
  - No standard user experience
  - Supports challenge response methods (APOP for example) and simple verification

Authentication Authority

Determines how to authenticate a user

- New attribute of a user record
- Apple has defined four major types for this attribute in Jaguar
  - Basic
  - Basic-Specific
  - ApplePasswordServer
  - Kerberos
- There will be more in the future—stay tuned

Example Values

Format is [version];[tag];[tag-data]

Attribute Value	Authentication Method Used
empty	Legacy behavior
“1.0;basic;”	Legacy behavior
“1.0;basic-specific;MD5”	MD5 hash stored in user record
“1.0;ApplePasswordServer;[data]”	Use Apple’s Password Server
“1.0;Kerberos;[realm name]”	Use Kerberos for this user

Password Server

- Password Server included with Jaguar Server
- Based on SASL (Simple Authentication and Security Layer)
- Provides password verification
    - No network password recovery
- Enforces password policies
    - Minimum length, expiration

Password Server Usage

Client accessing service

Mac OS X Client

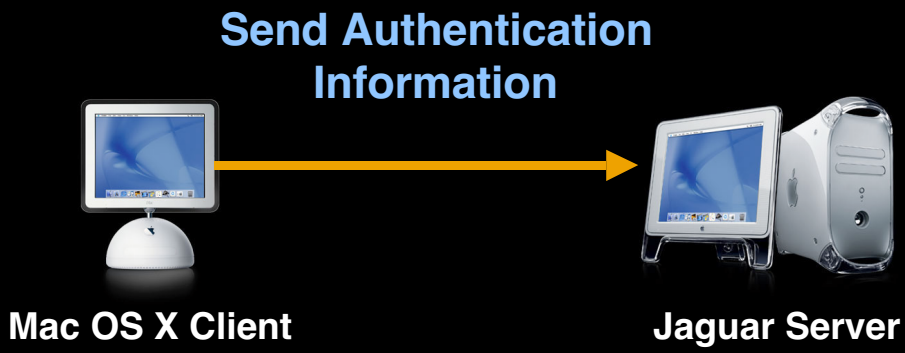
Jaguar Server

Directory Server

Password Server

Password Server Usage

Step 1

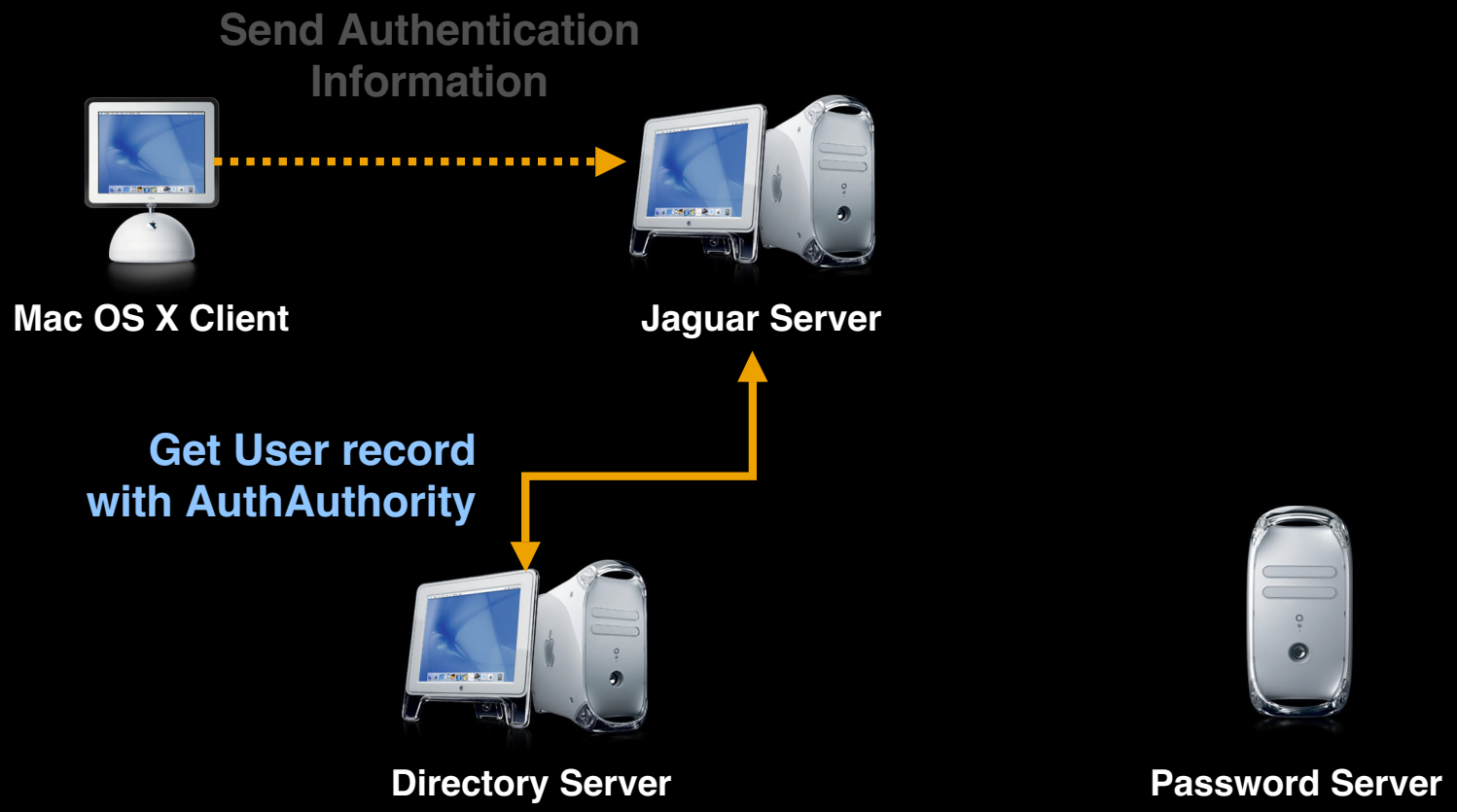



Directory Server


Password Server

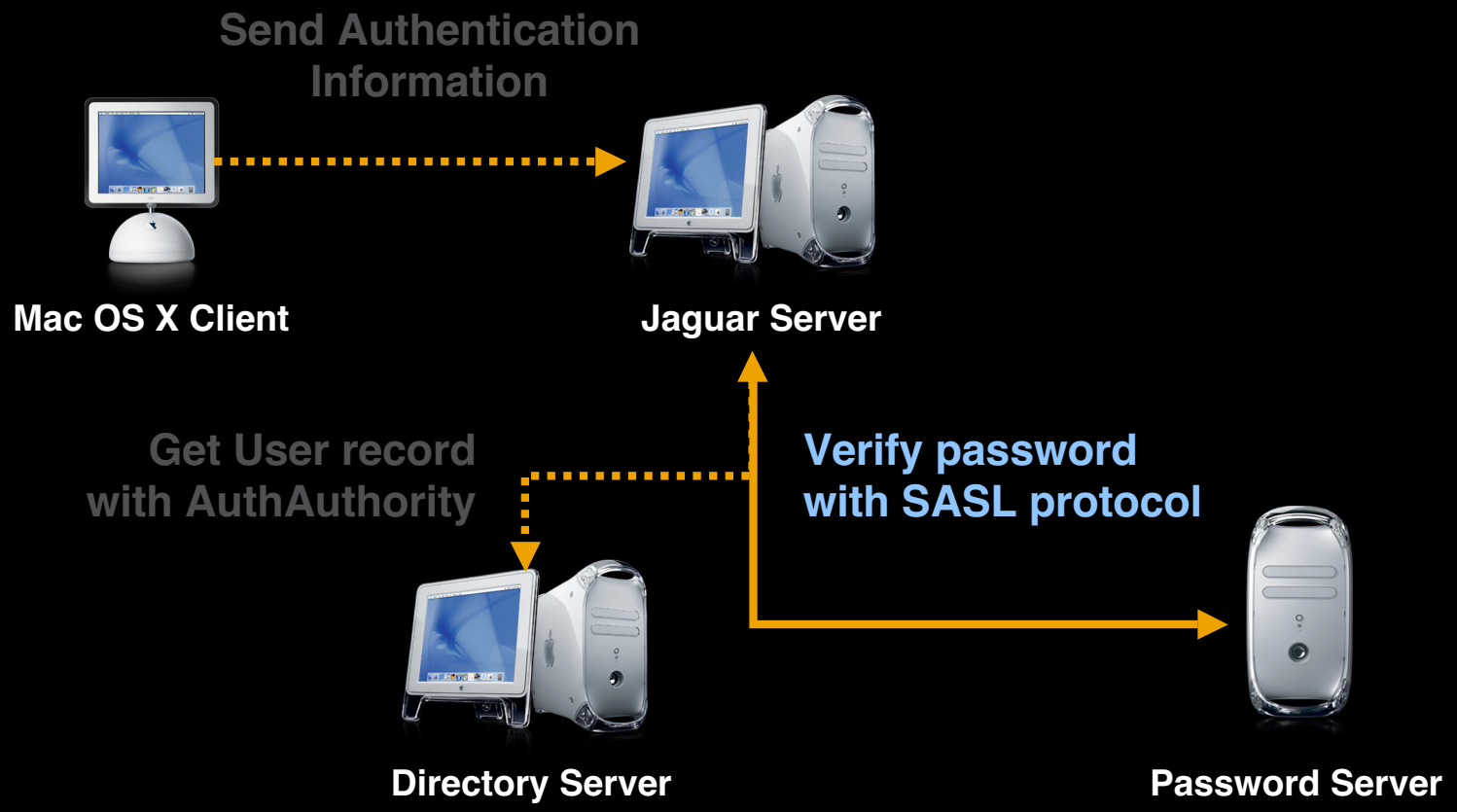
Password Server Usage

Step 2



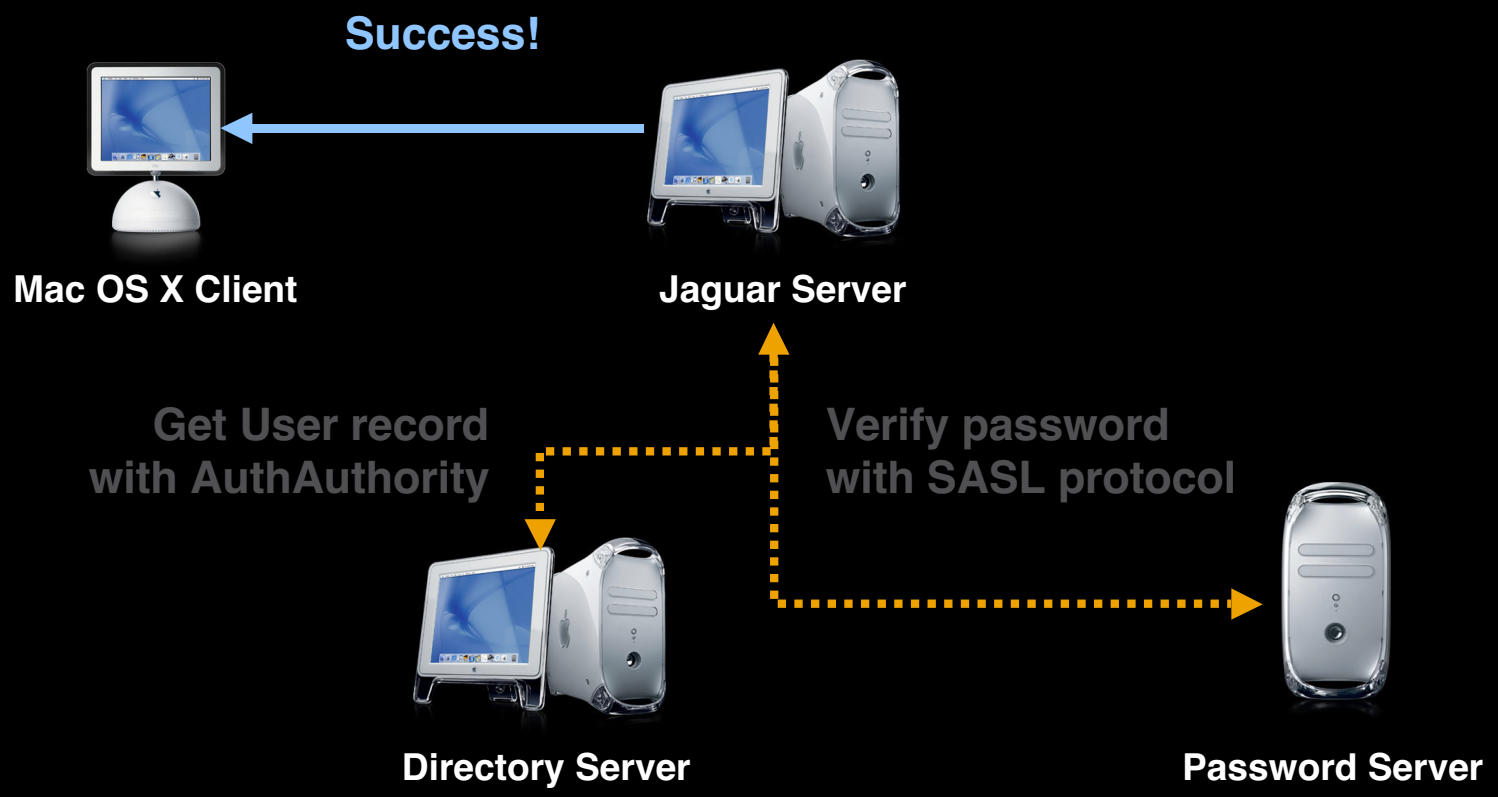
Password Server Usage

Step 3



Password Server Usage

Step 4



Authentication Methods

- SASL Server uses the RFC defined SASL methods via TCP/IP
- Authentication methods supported
  - Standard SASL methods
  - Plus some new Apple additions
    - MD5, CRAM-MD5, WebDAV Digest, 2-way Random, DHX (AFP), APOP, NT/LAN Manager, MS Chap II, SHA-1
- Secure set password operation

Authentication Review

- Jaguar will support more than crypt
- Apple will provide support for multiple methods
- Adopt a password verification API to insulate your product from password verification specifics
    - Example: password server use will be transparent if proper API is adopted

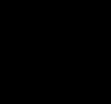
Service Discovery

Service Discovery

- Network Service Location (NSL) is Apple's high-level API for finding services
  - Provides both raw-data and a high-level human interface APIs
  - Automatically supports many service discovery protocols
- Mac OS X Finder "Connect to Server" menu item uses this API

Service Discovery

- In Jaguar, NSL entirely based on Open Directory
  - Allows browsing of static and dynamic directories (LDAP and Rendezvous)
  - Extensible by Apple and developers
- New plug-ins in Jaguar
  - AppleTalk, SLP, Rendezvous service discovery
- New logical structure
  - Simple local and full network



Service Discovery

- Existing applications using NSL automatically benefit from Directory Service plug-ins
    - No code changes required
- NSL UI transparently supports Rendezvous
    - Seamless conversion from Rendezvous to URLs

Service Registration

Add service registration to your networking product

- Augments your existing service registration strategy
- Continue to register with legacy service discovery protocols for maximum compatibility
    - Add a preference to your application to enable/disable different registration methods

NSL Summary

- Use NSL to find services
  - Easy API, standard user experience
  - Automatic support for many different service discovery protocols
  - Can be used for both raw data and simple HI
- Add Rendezvous service registration to your product
  - Apple's strategy moving forward
  - Allow customer maximum choice of protocol for their network

Demo

Jason Townsend

Summary

David M. O’Rourke

Summary

- Open Directory
  - Directory Access, Directory Servers, Directory Tools
  - Open Source today as part of Darwin
- Jaguar Features
  - LDAPv3 and enhancements
    - Read/write, DHCP integration, centralized management, complex schema support

Summary

- Jaguar Features
  - Directory Proxy
    - Allows remote access for all Directory Service API-based applications
  - Authentication changes are coming
    - Crypt may not be there
    - Adopt a password verification API
      - Security Framework, PAM, or Directory Services

Summary

- Jaguar Features—Service Discovery (NSL)
  - Network Service Location for finding services on the network
    - Uses all Directory Service plug-ins for static and dynamic content
  - New NSL organization
  - Add Rendezvous registration to your product

Summary

- Jaguar Server Features
  - Server will include a new SASL-based Password Server
- Jaguar will also offer support for Kerberos

For More Information

- Authentication Documentation
  http://asg.web.cmu.edu/sasl/
  http://www.kernel.org/pub/linux/libs/pam/
- Directory Services and Network Service Location (NSL) APIs
  http://www.apple.com/developer
- Directory Services Open Source
  http://www.apple.com/darwin

Roadmap

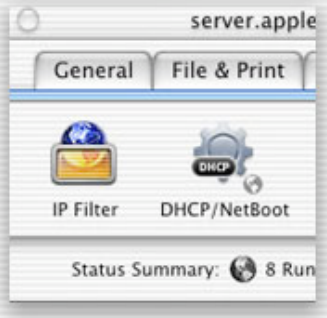
103 Open Source, Apple, and You	Civic **Tue., 2:00pm**
110 Security: Authorization in Mac OS X	Civic **Wed., 2:00pm**
811 Zero Configuration Networking	Hall 2 **Thurs., 2:00pm**
814 Kerberos in Mac OS X	Room C **Thurs., 5:00pm**

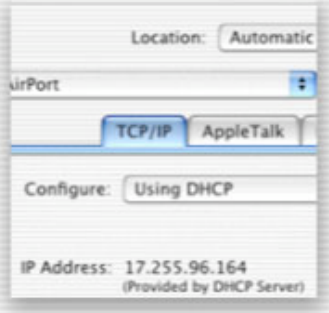
Who to Contact

Tom Weyer
Network and Communications Evangelist
weyer@apple.com

http://developer.apple.com/wwdc2002/urls.html

Q&A





Tom Weyer
Network and Communications Evangelist
weyer@apple.com

http://developer.apple.com/wwdc2002/urls.html


WWDC2002


WWDC2002


WWDC2002